Raytheon **ECS Project**

Engineering Technical Directive **No. 01-013**

Subject: Rexec, Rsh, and Telnet default account accessible **7 November 2001**

The following directive is issued to the PVC and VATC.

Issue: It is a security risk to leave the Rexec, Rsh, and Telnet default accounts (such as **Guest** and **lp**) accessible. Default accounts through these remote services allow attackers easy access to remote systems.

Fix: 1. Disable the Rexec, Rsh or Telnet default account or change the password to something difficult to guess for the following Hosts:

PVC	VATC
198.118.220.26	198.118.232.12
198.118.220.41	198.118.232.14
198.118.220.42	198.118.232.28
198.118.220.43	198.118.232.29
198.118.220.57	198.118.232.30
198.118.220.60	198.118.232.43
198.118.220.62	198.118.232.44
198.118.220.66	198.118.232.49
198.118.220.150	198.118.232.53
198.118.220.153	198.118.232.54
198.118.220.154	198.118.232.55

Testing: Verify that the Rexec, Rsh, and Telnet default accounts are not easily accessible.

Implementation: Unix: Disable login access to this Unix account if it is not needed.
To remove login access for a Unix account:

a) Edit the /etc/passwd file.
b) Locate the account.
c) Place an * (asterisk) in the password field.
d) Place the string /bin/false in the shell field. An example of the /etc/passwd entry for a disabled Guest account should resemble the following: guest:*:2311:50:Guest User:/home/guest:/bin/false
e) Save and exit the file.

Point of Contact: Mel Hudson, tele: 301/925-1099, email: mhudson@eos.east.hitc.com

Approved By: V. Maclin
Director, Systems Engineering

Reference CCR: 01-0860

--------End of Directive-------